

**WEIL, GOTSHAL & MANGES LLP**

SUITE 100  
1501 K STREET, N.W.  
WASHINGTON, D.C. 20005  
(202) 682-7000  
FAX: (202) 857-0940

BRUCE H. TURNBULL  
DIRECT LINE 202-682-7070  
bruce.turnbull@weil.com

AUSTIN  
BOSTON  
BRUSSELS  
BUDAPEST  
DALLAS  
FRANKFURT  
HOUSTON  
LONDON  
MIAMI  
MUNICH  
NEW YORK  
PARIS  
PRAGUE  
SILICON VALLEY  
SINGAPORE  
WARSAW

March 1, 2004

RECEIVED

MAR - 1 2004

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

Federal Communications Commission  
Office of the Secretary  
Attn: Broadcast Flag Certifications  
c/o Natek, Inc.  
236 Massachusetts Avenue, NE  
Suite 110  
Washington, DC 20002

**Re: Digital Content Protections Technologies and  
Recording Methods to be Used in Covered  
Demodulator Products – HDCP Technology**

Dear Sir or Madam:

Enclosed please find a Broadcast Flag Certification submission on behalf of Digital Content Protection, LLC ("DCP").

Please do not hesitate to contact me at the telephone number above if you have any questions concerning this submission.

Sincerely,



Bruce H. Turnbull

cc: Chief, FCC Media Bureau

**Before the  
Federal Communications Commission  
Washington, D.C. 20554**

In the Matter of: )  
 )  
Digital Content Protection Technologies and )  
Recording Methods to be used in Covered )  
Demodulator Products )  
 )  
**HDCP Technology** )

**CERTIFICATION OF  
DIGITAL CONTENT PROTECTION, LLC  
FOR APPROVAL OF ITS  
HIGH BANDWIDTH DIGITAL CONTENT PROTECTION (“HDCP”) AS  
AN APPROVED DIGITAL OUTPUT PROTECTION TECHNOLOGY**

**Table of Contents**

Certification Statement .....	3
Introduction and Summary .....	3
Responses to Specific Requirements .....	4
I. General Description .....	4
II. Detailed Analysis of the Level of Protection Afforded by HDCP Technology .....	5
A. DCP License-Based Protections .....	5
1. General .....	5
2. Broadcast Flag-Related Protection .....	5
3. Patents .....	5
B. Applicability of Functional Criteria .....	6

1. Level of Security.....	6
2. Scope of Redistribution Control .....	6
3. Means of Authentication.....	7
4. Renewability, Ability to Revoke Compromised Devices .....	8
5. Interoperability.....	8
III. Information on Approval and Licensing of HDCP Technology.....	8
A. Content Owners and Other Content Protection System Proprietors .....	8
B. Product Manufacturers .....	9
C. Consumers.....	10
IV. License Terms and Conditions .....	10
V. Other Considerations.....	15

Exhibits:

1. List of HDCP Licensees
2. HDCP License Agreement
3. HDCP Component License Agreement
4. HDCP Reseller Associate Agreement
5. HDCP Content Participant Agreement
6. High-Bandwidth Digital Content Protection System (Revision 1.1)
7. Upstream Link for High-Bandwidth Digital Content Protection (Revision 1.00)
8. Upstream Link for High-Bandwidth Digital Content Protection Revision 1.0 Erratum

## **Certification Statement**

In response to the Public Notice issued on January 23, 2004, by the Federal Communications Commission ("FCC" or "Commission"), the Digital Content Protection, LLC ("DCP") hereby submits its certification that the High bandwidth Digital Content Protection ("HDCP"), developed by Intel Corporation ("Intel") and licensed, under authorization from Intel, by DCP, meets the requirements for an Authorized Digital Output Protection Technology set forth in the Commission's regulations at 47 C.F.R. §§ 73.9000-9008 for the protection of Unscreened or Marked Content originating as digital terrestrial broadcast video content and, accordingly, requests the Commission's approval of HDCP for such purposes.

## **Introduction and Summary**

This document describes several aspects of the HDCP technology and its associated license agreements, but does not replace, amend, supercede or otherwise qualify the actual language set out in the HDCP technology specification and its associated license agreements. Further, this document and the descriptions herein are not intended to suggest that the HDCP technology, its associated license agreements, and the technology and licensing approaches therein should be used by the Commission as "models" when considering other certifications.

HDCP is a technology that protects the digital transmission of uncompressed digital video content from a consumer source device to a consumer display device. No copying is permitted for content protected with HDCP, and outputs from display devices are strictly limited.

HDCP was initially designed (beginning in 1999) in direct response to the expressed concerns of content companies that there was no system available to protect the delivery of video content from a computer to a display. This concern was magnified with the advent of the Digital Video Interface ("DVI"), which allowed high speed *digital* connections between computers and displays. In response, Intel developed HDCP to protect digital content delivered from a computer to a display over the DVI interface. For Intel, the development and licensing of HDCP was, and remains, a digital-market enabling activity, and the content community was quick to support HDCP for this purpose.

With the acceptance of HDCP over DVI protection in the computer environment, Intel supported efforts to have HDCP over DVI approved for use in the consumer electronics ("CE") environment as well, as information technology ("IT") and CE interoperability is an important Intel objective. As part of those efforts, Intel agreed to authorize DCP to license HDCP for use in both IT and CE implementations of DVI on the same market enabling terms and conditions (including the same "necessary claims" patent license grant directly from Intel) and then updated the HDCP specification to accommodate the HDMI interface (including audio applications in that interface – essentially DVI plus audio extensions), which is backward compatible with DVI and can be implemented in both IT and CE products. For Intel, the entire effort and its

willingness to extend its work into the CE environment was, and remains, an important part of its digital market enabling efforts (which also include Digital Transmission Content Protection (“DTCP”), Content Protection for Recordable Media (“CPRM”), etc.) designed to enhance consumer choice and flexibility in the digital home by providing some of the basic infrastructure necessary to support exciting new business models based on the delivery and consumption of premium digital entertainment content.

HDCP is an important element of an overall content protection architecture because it protects uncompressed content, which enables high resolution digital displays to receive and then display protected digital content without the need for resource intensive decompression capabilities. In the digital home, HDCP protects the important “last mile” in the protected digital environment, which is the link to the digital display.

Today, HDCP has been licensed by more than 85 companies, HDCP-enabled products are available in both IT and CE products, and products supporting HDCP are sold throughout the United States and elsewhere in the world. HDCP is widely supported, including for example as an approved output in the Cable Plug and Play DFAST License, supported by all of the motion picture studios in these proceedings, an approved digital output for DVD video content in the Content Scramble System license, and is an approved output for DTCP protected content as well.

To protect content delivered over the DVI and HDMI interfaces, HDCP utilizes a gender-based key distribution system (“KDS”) to provide authentication key exchange (“AKE”) between a transmitter and a receiver. The AKE provides a distinct, fixed 56-bit key for each pair of transmitter and receiver devices, which is then used with an 84-bit (key size and block size) block cipher to encrypt a fresh 64-bit random number to provide a 56-bit session key. The session key and block cipher provide a sequence of frame keys and authentication responses and other responses to ensure the continued synchronization of the transmitter and receiver cipher engines. Each frame key is used to initialize a stream cipher, which encrypts at most one frame of data. In addition, before each horizontal line of video data, the stream cipher engine is freshened (partially re-keyed) to limit the amount of ciphertext that is available to analyze the stream cipher under a single key to one line of video. The stream cipher is composed of a linear feedback shift register (“LFSR”)-based freshness generator, previously mentioned block cipher core, and output function layer. The stream cipher provides a very high encryption rate at a very modest resource cost suitable for uncompressed video data rates, producing 24-bit RGB pixels for each video clock.

## **Responses to Specific Requirements**

### **I. General Description**

As indicated above, HDCP is designed to deliver video (and, in the HDMI implementation, audio, whether accompanying video or transmitted independently) for the

purpose of viewing (and hearing, in the case of audio). Only uncompressed video is protected by HDCP technology. As such, HDCP is designed to be part of an overall consumer environment in which other technologies permit authorized copying or management of content in networked environments. HDCP is the “last link” in the chain before a consumer sees or hears the content. This enables the use of displays that do not themselves contain the expensive and rapidly evolving technologies for decompressing video, thereby allowing the display elements to be used for much longer periods of time, while electronics for decompression can be upgraded as part of non-display elements of a consumer’s system (whether computer-based or not).

## **II. Detailed Analysis of the Level of Protection Afforded by HDCP Technology**

### **A. DCP License-Based Protections**

#### **1. General**

As indicated above, HDCP is an encryption-based technology that protects uncompressed video delivered to a digital display. The HDCP license contains compliance rules that prohibit HDCP from being used to copy and/or redistribute content, except in limited cases to another digital display over a repeater. (*See* Exh. 2, HDCP License Agreement, Exh. C.) The HDCP compliance rules are by the far the simplest of all the content protection technology compliance rules that Intel has participated in (*e.g.*, DTCP, CRPM) because HDCP is a single purpose technology that protects the last link out to a consumer’s display (*See* Exh. 2, HDCP License Agreement, Exh. D.)

The HDCP license also contains robustness rules that detail how HDCP must be implemented in order to resist attempts to circumvent the HDCP protection. The HDCP robustness rules are similar to other well established robustness rules (*e.g.*, DTCP, Cable Plug and Play DFAST, CPRM) in almost all material respects.

#### **2. Broadcast Flag-Related Protection**

HDCP can play a very important part in both the protection of digital broadcast television, and in consumer enjoyment thereof because it provides protection between the digital receiver and the consumer’s display. As indicated above, HDCP cannot be used to make copies and cannot be used to redistribute the content except to another digital display through a repeater.

#### **3. Patents**

HDCP is a technology developed solely by Intel. All patent claims owned by Intel that meet the Adopter License definition of “Necessary Claims” are licensed. (*See* Exh. 2, HDCP License Agreement § § 1.34, 2.1.) Specific patents are not listed in the license. The “Necessary Claims” approach to patent licenses is a common one used by technology industries, including specifically content protection technology licenses (*see, e.g.*, the Content Scramble System (“CSS”) License for DVD Video). This approach assures the licensee that it has access

to all claims that are, in fact, owned by the technology developer and “necessary” in order to implement the technology. In this context, a licensee need not fear a patent infringement claim being brought by the licensor against it sometime after signing the license for a patent that is not identified on an initial list but is in fact “necessary,” avoiding the cost, complexity and uncertainty associated with determining as a legal matter which patents in a large portfolio might in fact be “necessary.” Further, patents that are issued to Intel after the date of the license, but that contain “Necessary Claims,” are automatically added to the license. Patent issues as they relate to other license terms are discussed further below.

## **B. Applicability of Functional Criteria**

### **1. Level of Security**

HDCP is an effective method for protecting uncompressed digital video content for display only (or, in the case of audio, listen-only) purposes. First, HDCP uses the following technical elements to keep content from being intercepted for unauthorized purposes: authentication between source and display devices and content encryption at the source and decryption at the display. Second, HDCP’s specifications, including the specification for its encryption algorithm, are publicly available on DCP’s website,<sup>1</sup> and have been publicly available since February 2000 (with an updated specification posted in June 2003). Secrets requiring confidential or highly confidential treatment by licensees are at the minimum necessary to maintain an encryption-based system, that is, only cryptographic values and keys are required to be maintained as secret. Third, because keys are specific to each HDCP-enabled product, any compromise of these values can be remedied through revocation of the keys for that specific product.

The encryption element of HDCP security is described above (see Introduction and Summary) and below (Section II.B.3, “Authentication”). It is of note that certain elements of the system were dictated by the export restrictions in place at the time of its development, and updating features such as the key length to match evolution in export permissions is not possible due to the fact that portions of HDCP are enabled in hardware products that are themselves not readily capable of upgrading. Nevertheless, the cryptographic strength of HDCP is well matched to the purpose of the protection – which is to enable display of content for consumer enjoyment, not to protect individual secrets as might be the case in a financial transaction.

### **2. Scope of Redistribution Control**

With respect to the redistribution control purposes of the Commission’s Broadcast Flag proceeding, the HDCP license prohibits copying an HDCP encrypted stream, and further prohibits redistribution except to another digital display using a repeater. From a purely technical and practical perspective, HDCP encrypted content is fully decompressed digital video

---

<sup>1</sup> The URL for DCP is <http://www.digital-cp.com>

content, meaning that from a quantity of data perspective, it is not data readily suitable for copying and redistribution.

### **3. Means of Authentication**

As noted above, HDCP uses an explicit authentication system to ensure that receiving products are HDCP-enabled and authorized. A detailed description is contained on pages 9-33 of the HDCP Specification document (Exhibit 6 to this certification). The following excerpt from the introductory sections of the authentication portion of the HDCP specification document provides a basic description of the process:

#### **“2. Authentication**

“The HDCP Authentication protocol is an exchange between an HDCP Transmitter and an HDCP Receiver that affirms to the HDCP Transmitter that the HDCP Receiver is authorized to receive HDCP Content. This affirmation is in the form of the HDCP Receiver demonstrating knowledge of a set of secret device keys. Each HDCP Device is provided with a unique set of secret device keys, referred to as the Device Private Keys, from the Digital Content Protection, LLC. The communication exchange, which allows for the receiver to demonstrate knowledge of such secret device keys, also provides for both HDCP Devices to generate a shared secret value that cannot be determined by eavesdroppers on this exchange. By having this shared secret formation melded into the demonstration of authorization, the shared secret can then be used as a symmetric key to encrypt HDCP Content intended only for the Authorized Device. Thus, a communication path is established between the HDCP Transmitter and HDCP Receiver that only Authorized Devices can access.

#### **“2.1 Overview**

“Each HDCP Device contains an array of 40, 56-bit secret device keys which make up its Device Private Keys, and a corresponding identifier, received from the Digital Content Protection, LLC. This identifier is the Key Selection Vector (KSV) assigned to the device. The KSV is a 40-bit binary value.

“The HDCP Authentication Protocol can be considered in three parts. The first part establishes shared values between the two HDCP Devices if both devices have a valid Device Key Set from the Digital Content Protection, LLC. The second part allows an HDCP Repeater to report the KSVs of attached HDCP Receivers. The third part occurs during the vertical blanking interval preceding each frame for which encryption is enabled, and provides an initialization state for the HDCP Cipher for encrypting the HDCP Content within that frame.”



#### **4. Renewability, Ability to Revoke Compromised Devices**

HDCP allows a HDCP transmitter to identify compromised devices and prevent the transmission of HDCP content to such devices via HDCP System Renewability Messages (SRM). (See Exh. 6, High-Bandwidth Digital Content Protection System (Revision 1.1) § 5.) The SRM contains a list of revoked HDCP Receivers as identified by their Device Keys Sets. HDCP Receivers are issued a unique set of Device Private Keys, matched with a non-secret identifier (the KSV), referred collectively as the Device Key Set.

Because revocation of products is a significant act not taken lightly by any party, there is a careful process that must be employed before any product's Device Key Set is actually revoked as described in section 7 of the HDCP Adopter Agreement. (See also Exh. 2, HDCP License Agreement, Exh. A § 3.) Where the licensee agrees that revocation is the correct approach in a particular instance (e.g., Device Keys Sets are lost or stolen and everyone agrees revocation is appropriate), the revocation decision is immediate. Where a licensee does not agree, however, that revocation is appropriate, the HDCP license sets forth a more elaborate process including the involvement of an outside, neutral arbitrator to make the critical decision as to whether a key has, in fact, been compromised such that revocation is the appropriate step.

Once a decision to revoke keys is taken, the technical process for revoking the key is accomplished by the propagation of HDCP SRMs through media and transmitted content. Devices that use HDCP as an approved output are responsible to make sure that revocation messages are processed during authentication and that the secure status of the HDCP device is checked.

#### **5. Interoperability**

As with other content protection systems relying on encryption and authentication, HDCP is a fully interoperable system for products that are licensed by DCP and implement HDCP. Although the DVI and HDMI interfaces have different physical connectors, the underlying DVI protocols are interoperable and connection adaptors are available so that consumers can connect DVI and HDMI inputs/outputs to take advantage of the underlying common DVI interface.

### **III. Information on Approval and Licensing of HDCP Technology**

#### **A. Content Owners and Other Content Protection System Proprietors**

Since HDCP was designed for display-only purposes, content companies have for the most part been very positive about its use and deployment in computer and CE-type products.

With regard to the use of HDCP for broadcast flag-related purposes, Intel was an active participant in the Broadcast Protection Discussion Group and follow-on discussions related to the Broadcast Flag. As part of that process, Intel proposed that HDCP would be a technology meeting the broadcast redistribution protection requirements that were discussed in that group. During the BPDG discussions, all MPAA members participating in the BPDG indicated their agreement with that assessment. That view was confirmed to the Commission in comments filed in the initial Broadcast Flag rulemaking. *See* Joint Comments of Motion Picture Association of America *et al.*, Docket MB 02-230, at 26 (Dec. 6, 2002).

HDCP has also been approved by other content protection systems for use with content that is initially protected using those other technologies. For example, (i) the DVD Copy Control Association, Inc. has approved use of HDCP as an authorized secure digital output for playback of DVD video content protected using the Content Scramble System; (ii) HDCP is an approved digital output in DFAST License, which is part of the “plug and play” agreement between cable operators and consumer electronics manufacturers, and is included in regulations issued by the Commission aimed at ensuring that consumers are able to get MSO provided set top boxes with protected digital outputs; (iii) 5C has approved HDCP as an approved digital output for DTCP protected content; (iv) 4C Entity, LLC has approved HDCP as an Authorized Secure Digital Output for video content protected with 4C’s Content Protection for Recordable Media; and (v) JVC has approved HDCP as an authorized output for content protected through JVC’s D-VHS protection requirements, including content that is copied by consumers using the “regular” D-VHS protections and content that is released on prerecorded D-VHS cassettes using JVC’s “D-Theater” protections.

Each of the above approvals, for use of HDCP in relation to content initially protected with other forms of content protection technology, involved extensive interaction between the proprietors of those other technologies and content companies. In the DVD CCA case, for example, the approval of HDCP-protected digital outputs involved a formal process in which all MPAA-member companies participated in DVD CCA’s Content Protection Advisory Council and voted in favor of the amendment to CSS’ specifications necessary to permit HDCP outputs and in which six content company officials serving on the DVD CCA Board of Directors also voted in favor of approving HDCP-protected outputs.

In short, HDCP has been almost universally accepted as an effective protection technology for transmitting uncompressed video content for display purposes.

## **B. Product Manufacturers**

To date, 85 product manufacturers have been licensed to produce HDCP compliant devices. Products implementing HDCP are offered in the U.S. consumer marketplace by a number of companies.

### **C. Consumers**

Although HDCP is not a copy or link layer transport technology, HDCP does enable the consumer to enjoy premium content seamlessly. HDCP is deployed for use at points in the consumer environment when a consumer is going to view (and hear) the content, rather than at a point when the consumer is enabling a networked application or attempting to make a copy of the content. HDCP therefore operates “invisibly” to the consumer. That is, HDCP does nothing to alter the normal viewing or listening experience of the consumer, and is not used when the consumer is doing something else with the content. Where a consumer is going to enable a network application or make an authorized copy, HDCP is not used, and the consumer experience should not be unaffected by the high bandwidth and “no copies allowed” features of HDCP protected interfaces.

The use of DVI connections is now well-established in the computer environment, and consumers have had no difficulty adapting their systems for such uses. In the HDMI case, the CE industry has worked to ensure that the physical connectors used for HDMI are of a type familiar to consumers and easily used in connection with CE-type products. HDCP itself, however, is not, connector dependent.

### **IV. License Terms and Conditions**

In response to the Commission’s request for information concerning license terms and conditions, DCP is submitting as appendices to this document, the following licenses offered in connection with HDCP technology: HDCP License Agreement (Exhibit 2), HDCP Component License Agreement (Exhibit 3), HDCP Reseller Associate Agreement (Exhibit 4), HDCP Content Participant Agreement (Exhibit 5), High-Bandwidth Digital Content Protection System (Revision 1.1) (Exhibit 6), Upstream Link for High-Bandwidth Digital Content Protection (Revision 1.00) (Exhibit 7), Upstream Link for High-Bandwidth Digital Content Protection Revision 1.0 Erratum (Exhibit 8). For the Commission’s further understanding DCP describes below certain elements of its licenses.<sup>2</sup>

---

<sup>2</sup> DCP does not believe as a matter of principle that the government should be involved in reviewing private license agreements, or otherwise in determining what constitutes a “reasonable and non-discriminatory license.” Certainly such review challenges the very limits of the Commission’s jurisdiction and raises a host of related legal issues. To be sure, the Commission’s mandate with respect to broadcast flag content is to protect the content consistent with both the compliance requirements (prohibit indiscriminate redistribution to the public) and the robustness requirements (ordinary user standard) established by the Commission in these proceedings, and there is no Commission mandate to implement any particular content protection technology to that end. DCP believes that self certification with respect to the compliance and robustness requirements established by the Commission is the course of action most consistent with the general principle that content protection solutions should be the result of voluntary industry agreements and not government mandates. In this context, while the Commission has nevertheless expressed an interest in reviewing the content protection qualities of a technology,

First and foremost, the HDCP license is a digital market enabling technology license. It is offered for the purpose of helping build out a protected digital environment that can support new businesses and new products for consumers. In this context, DCP notes the following. First, the HDCP license reflects a well-developed approach to content protection technology licensing that includes “necessary claims” license grants and reciprocal non-asserts. This licensing approach reflects the cross industry collaboration on similar efforts over the years, beginning with the CSS License for DVD Video, and including the licenses for DTCP, CPRM and other content protection technologies. Second, as an enabling effort, the fees associated with the HDCP technology do not reflect full market rates, and are offered with an eye toward cost effective implementation and cost recovery so that DCP can sustain its licensing activities long term for the benefit of all who invest in the use of HDCP. The enabling nature of this technology offering reflects the fact that while content protection has become a necessity part of the digital

---

license terms and conditions not directly related to the content protection qualities of a technology (i.e., robustness and compliance rules) should in all instances be a matter of private contract left to market participants. Indeed, DCP notes that the Commission has not adopted a requirement that an approved technology in fact even be licensed to the public, meaning that from a fundamental philosophical perspective, the Commission must recognize the principle that private intellectual property holders exercise ultimate discretion with respect to licensing matters, and private parties in the marketplace decide what is “reasonable,” and technology developers are wholly free to “discriminate” if they choose. Indeed, under the current review criteria, the Commission might approve a wholly proprietary technology that is not offered to any third party, but reject a technology that is offered to the public on the basis that Commission deems some of its terms “unreasonable” or “discriminatory” despite the fact that its content protection qualities and enforcement mechanisms may be superior. In this light, the Commission’s consideration should *not* be whether implementers would desire to license a given solution, but whether an implementer that so desires should be precluded from doing so in the context of DTV protection, a determination which should be made, if at all, only on the basis that the technology provides less than adequate protection. Consistent with these principles, DCP does not believe that the Commission should approve or disapprove technologies on the basis of the terms on which they may or may not be offered to third parties, and certainly not on the basis of terms and conditions not directly related to content protection (i.e., compliance and robustness). Government regulation of private contracts is not the path to consumer choice. To be sure, the Commission is *not* reviewing the license terms and conditions associated with more general technologies necessary or desirable as a matter of *choice* to build a digital television broadcast receiver or related product, including but not limited to MPEG and other desirable compression and decompression technology licenses, IEEE 1394 and other digital transport protocol licenses, physical and electronic media formats, and the multitude of other basic technology licenses relevant to building devices that might be used to receive, copy, distribute, or playback digital broadcast television. DCP sees no justification for the Commission selectively reviewing content protection technology licenses that are voluntarily offered to the public for adoption at the discretion of the implementer, for issues wholly unrelated to the broadcast flag mandate of protecting digital broadcast television.

infrastructure to promote the development of new digital goods and services, content protection is not a “feature” for which consumers will pay a premium.

With those general statements as introduction and with reference to the attached licenses for more detail on each element, DCP offers the following brief descriptions of certain important elements of its licenses:

(1) License structure. DCP offers the following types of licenses, designed to allow specific types of licensees to adopt licenses specifically suited to their particular circumstances. First, the basic HDCP License Agreement (or “Adopter Agreement”) is designed for companies that intend to develop, manufacture and sell products that fully implement HDCP in accordance with the HDCP Specification, Compliance Rules and Robustness Rules. (See Exh. 2.) Second, the HDCP Component License Agreement is tailored to permit companies to make components incorporating HDCP functionality for sale to other HDCP licensees for inclusion in full HDCP implementations. (See Exh. 3.) Third, the Reseller Associate License permits companies that sell (and, in most cases, buy) HDCP-enabled components (such as semiconductors) but themselves have no need for access to the technology to engage in their businesses while ensuring that their customers are HDCP licensees and that, hence, the components will be incorporated into full HDCP implementations in accordance with the HDCP Specification, Compliance and Robustness Rules. (See Exh. 4.) Finally, DCP offers a Content Participant Agreement that permits content companies that choose to enter the agreement to gain certain rights, such as third party beneficiary rights to (a) seek injunctive relief with respect to HDCP implementations that materially fail to satisfy the requirements of the HDCP Adopters License, (b) initiate and participate in the key revocation processes, and (c) participate in the process of making and/or approving changes to the HDCP License, Specification, Compliance and Robustness Rules. (See Exh. 5.)

(2) Basic license/scope of use. Each license is specific to the HDCP technology. For example, the Adopter Agreement conveys a nonexclusive worldwide license to Intel-owned Necessary Claims and to Intel and DCP owned trade secrets and copyrights with respect to HDCP and the HDCP Specification. (See Exh. 2 § 2.1.) Each of these licenses permits the making (or having made), using, and transferring (selling, importing, etc.) of HDCP implementations, subject to compliance with the HDCP Specification, Compliance rules, and Robustness rules. The coverage of the licensed technology is limited to the actual implementation of the HDCP technology, as HDCP technology is disclosed in the HDCP Specification. Exceptions and clarifications to the scope of the licensed technology are spelled out in the definition of “Necessary Claims” (see Section 1.34) and a separate “limitations” section (see Section 2.4).

(3) Confidentiality. Since the HDCP Specification is public, there is very little that a Licensee is required to keep confidential other than the cryptographic keys that are the core of this cryptographically-based authentication technology. (See, e.g., Exh. 2, HDCP License Agreement, Exh. B.)

(4) Compliance Requirements. As with other content protection licenses, a licensee must comply with the requirements set forth in the HDCP Specifications, Compliance Rules, and Robustness Rules.

(5) Individual Privacy. The HDCP Adopter Agreement specifically prohibits an Adopter from using any portion of the HDCP Specification or related keys or cryptographic information “for the purpose of identifying any individual or creating, or facilitating the creation of, any means of collecting or aggregating information about an individual or any device or product in which HDCP, or any portion thereof, is implemented.” (See Exh. 2 § 6.1.)

(6) Necessary Claims. The HDCP patent license provides a license from Intel to all Intel patent claims that are “necessary” to implement the HDCP technology, with specific limited exclusions for technologies not directly related to HDCP (e.g., codecs, interface technology, watermark technology, semiconductor technology, etc.). (See Exh. 2 § § 2.1, 2.4.) In this way, Adopters are assured that they have licenses to all relevant Intel patent claims as defined in the relevant agreements.

(7) Reciprocal Non-Assertion. In partial consideration of the market-enabling license terms offered by DCP (and Intel with respect to necessary claims license grants), licensees (including signers of the content participant agreement) agree not to assert any “necessary claims” they might have against DCP, its Founder, and HDCP licensees, but only with respect to HDCP implementations. (See Exh. 2 § 2.2; Exh. 5 § 2.2.) These reciprocal non-asserts remove barriers to system participation and promote competition within the system based on product features and functions. There are no other constraints or limitations on an Adopter’s ability to use and enforce patent claims that are “necessary claims” in the HDCP context where such claims are relevant to other technologies or applications, or even against another licensee if that licensee has breached its non-assert with respect to the first. As a general principle, including reciprocal non-asserts in conjunction with a patent license grant is a very common patent licensing practice, in industry consortia, industry standards activities, and in private strategic licensing activities. In market-enabling efforts like those engaged in by Intel in the field of content protection, reciprocal non-asserts create access to a “system”<sup>3</sup> wherein all of the voluntary participants are free to develop products without fear of infringement claims brought by the other participants in the system. Competition among participants is therefore based on innovation with respect to product functions and features and not on the underlying technology that is needed for participation and interoperability in the system (in this case, the HDCP source and display).

---

<sup>3</sup> In the case of HDCP, the “system” consists of interoperable source devices that encrypt and transmit, and display devices that decrypt and display. The system includes more than just interoperable technology components, however, because participation in the “system” means participating devices get access to all of the content that is allowed to flow over the HDCP protected link, including but not limited to cable content, DCP protected content, DVD Video content, etc

Creating a level playing field for participants in a market-enabling effort is an important element to the success of such an effort, both from a fairness perspective and from the very real consideration that licensors in a market-enabling effort are not in a position to indemnify licensees against patent infringement claims. Content protection market-enabling structures simply do not support indemnity obligations, but participants in such a system have a reasonable expectation that they should be able to understand, in advance of making substantial investments in the system, what the actual licensing costs will be with respect to the system, at least with respect to the participants in the system. Allowing one participant in the system to sue other participants in that same system on the basis that they are implementing a different part of the system (e.g., source vs. display) undermines the overall system and a central purpose of the market-enabling licensing structure.

Another important practical consideration is the fact that the HDCP technology and its licensing structure was developed long before the commencement of the Broadcast Flag proceedings or even the industry discussions in the Broadcast Protection Discussion Group. At this point, more than 85 companies have licensed HDCP and have not only agreed to the market-enabling licensing structure offered by DCP, but many have relied on it in making participation investments in the HDCP system. In the private arena, where consideration of *all* licensing terms and conditions is not only appropriate but an essential and integral part of market-based technology selection, the HDCP technology and all of its associated license terms and conditions were duly considered and relied on when approving HDCP as an output for the assortment of conditional access technologies already identified above.

(8) Keys and Key Expiration. DCP issues device keys to its licensees that are using the appropriate parts of the technology where device keys are necessary. The renewal and revocation of keys is governed by specific elements of the agreements, and these matters are discussed in more detail elsewhere in this document.

(9) Changes. The Adopter Agreements permits changes to be made to the HDCP Specification, Compliance Rules, Robustness Rules and Procedural Appendix, but only where changes that implicate product design (a) do not interfere with the backward compatibility of HDCP (i.e., licensed products made prior to the changes must be compatible with licensed products made after the changes), and (b) do not materially increase the cost or complexity of implementation of the HDCP specification. Changes to fees may only be made in accordance with limitations spelled out in the Agreements. (*See, e.g.,* Exh. 2 § 5.1.) All changes, however, must be notified well in advance (with changes implicating product design generally requiring a 12-18-month advance notice prior to their effectiveness). (*See* Exh. 5 § 3.6(b).) Signers of the Content Participant Agreements also get rights to review and object to any changes that are material and adverse to the integrity or security of the HDCP technology, the operation of HDCP with respect to protecting audiovisual content against unauthorized output, transmission, interception or copying, or to their rights under the Content Participant Agreement. (*See* Exh. 5 Content Participant Agreement § 3.6(b).)

(10) Fees. Product manufacturers pay two types of fees under the HDCP agreements – annual administrative fees to cover the costs associated with license administration, and unit fees for certain products and/or devices to cover the costs associated with generating and delivering millions of unique keys to Adopters. (*See, e.g.*, Exh. 2, HDCP License Agreement, Exh. A §§ 1.1-1.2.) Both rates are set at levels below typical commercial rates with an eye to cost recovery in recognition of the market enabling purpose of the technology offering and the fact that consumers do not view content protection as an added feature of consumer products. The fees are set forth in the Procedural Appendix to the Adopter Agreement. Annual fees are set at \$15,000 per year for each licensee, and device key fees vary according to the number of keys ordered. Signers of the Content Participant Agreement and the Component License Agreement pay only annual fees, with Content Participants paying \$50,000 per year and Component licensees paying \$15,000 per year. (*See* Exh. 5, HDCP Content Participant Agreement, Exh. C; Exh. 3, HDCP Component License Agreement, Exh. A § 1.1.) Signers of the Reseller Associate Agreement pay no fees, annual or otherwise.

## **V. Other Considerations**

Although the Commission did not incorporate the “Associated Obligations” proposal that had been put forward in the Broadcast Protection Discussion Group process, DCP believes that the Commission may wish to consider using this concept in its final approvals of the technologies to be authorized for use in relation to demodulator products. Accordingly, DCP hereby proposes the following “Associated Obligations” for companies using HDCP technology in connection with a covered demodulator product:

When passing Unscreened Content or Marked Content to an output protected by HDCP, a Covered Product shall (a) carry any HDCP System Renewability Message delivered in association with such content to the HDCP Source Function and (b) verify that the HDCP Source Function is fully engaged and able to deliver protected content, which means (i) HDCP encryption is operational on such output, (ii) processing of the valid received System Renewability Message associated with such content, if any, has occurred as defined in the HDCP Specification and (iii) there is no HDCP Display Device or Repeater on such output whose Key Selection Vector is in such System Renewability Message.

\* \* \* \* \*




For the reasons contained in this certification submission, DCP respectfully requests that the Commission approved HDCP as an authorized digital output protection technology for use with demodulator products covered under the Broadcast Flag regulations.

Respectfully submitted,



Stephen P. Balogh  
President  
Digital Content Protection, LLC  
2111 N.E. 25th Avenue  
JF2-55  
Hillsboro, OR 91724-5961  
[stephen.p.balogh@intel.com](mailto:stephen.p.balogh@intel.com)  
503 264-8426

Intel Legal OK	
	02/27/04

## DCP/HDCP Appendices

List of HDCP Licensees.....	1
HDCP License Agreement.....	2
HDCP Component License Agreement.....	3
HDCP Reseller Associate Agreement .....	4
HDCP Content Participant Agreement .....	5
High-Bandwidth Digital Content Protection System Specification (Revision 1.1).....	6
Upstream Link for High-Bandwidth Digital Content Protection Specification (Revision 1.00).....	7
Upstream Link for High Bandwidth Digital Content Protection Specification Revision 1.0 Erratum .....	8

# DIGITAL CONTENT PROTECTION, LLC

• digital-cp.com

## Welcome to the Digital Content Protection, LLC

This organization licenses technologies for protecting commercial entertainment content.

### List of HDCP Licensees

#### HDCP License Agreement

A & R Cambridge, Ltd.  
Analog Devices, Inc.  
Anam Electronics Co., Ltd.  
ASTRODESIGN, Inc.  
ATI Technologies, Inc.  
Aurora Multimedia Corporation  
BenQ Corporation  
Brilliant Corporation  
Broadcom Corporation  
Christie Digital Systems Canada, Inc.  
Chroma ATE Inc.  
Chunghwa Picture Tubes, Ltd.  
Conexant Systems, Inc.  
Coretronic Corporation  
Daewoo Electronics Corporation  
Delta Electronics, Inc.  
Denon, Ltd.  
DWIN Electronics, Inc.  
Eastern Asia Technology Limited  
EchoStar Technologies Corporation  
Eizo Nanao Corporation  
Explore Microelectronics, Inc.  
Focus Enhancements  
Fujitsu General Limited  
Funai Electric Co., Ltd.  
Gefen, Inc.  
Genesis Microchip Inc.  
Harman International Industries, Inc.  
Harsper Co., Ltd.  
Hitachi, Ltd.  
Humax Co., Ltd.  
Hyundai Digital Technology Co., Ltd.  
InFocus Corporation  
Intel Corporation  
Japan Aviation Electronics Industry, Ltd.  
JVC-Victor Company of Japan, Limited  
Kaleidescape  
Key Digital Systems

LG Electronics, Inc.  
Linn Products Limited  
Loewe Opta GmbH  
Lumagen, Inc.  
Marantz Japan, Inc.  
Master Co., Ltd.  
Matsushita Electric Industrial Co., Ltd.  
Meridian Audio Limited  
MIK21 Co., Ltd.  
Mitsubishi Electric Corporation  
Motorola, Inc.  
MStar Electronic Semiconductor, Inc.  
NEC Corporation  
NEC-Mitsubishi Electric Visual Systems Corporation  
Nexgen Mediatech, Inc.  
ONKYO Corporation  
Pace Micro Technology PLC  
Philips Semiconductors GmbH  
Pioneer Corporation  
Premier Image Technology Corp  
projectiondesign  
Prokia Technology Co., Ltd.  
Quanta Computer, Inc.  
Quantum Data, Inc.  
ROHM Co.  
Runco International, Inc.  
Sampo Corporation  
Samsung Electronics  
Sanyo Electric Co., Ltd. Multimedia Company  
Scientific-Atlanta, Inc.  
Seiko Epson Corporation  
Sharp Corporation  
Sichuan Changhong Electric Co., Ltd.  
Silicon Image, Inc.  
SIM2 Multimedia S.P.A.  
Sony Corporation  
TAG McLaren Audio Ltd.  
Taiwan Thick-Film Industries. Corp.  
Tatung Co.  
TEAC Corporation  
Texas Instruments, Inc.  
Thomson Multimedia S. A.  
Toshiba Corporation  
ViewSonic Corporation  
Xiamen Overseas Chinese Electric Co., Ltd. (Xoceco)  
Yamaha Corporation  
Zinwell Corporation  
Zoran Corporation

#### **HDCP Component License Agreement**

MediaTek, Inc.

#### **HDCP Reseller Associate Agreement**

ACTE Components A/S  
All American Semiconductor of Florida, Inc.  
AMSC Co., Ltd.

Arrow Nordic Components AB  
ASCA Tech Co. Ltd.  
Axess Technology  
Century International, Inc.  
Fuji Electronics Co., Ltd.  
Gold Insignia Electronic Co., Ltd.  
HY-Line Computer Components Vertriebs GmbH  
Inno Micro Corporation  
Kanematsu Corp  
Komatsu TriLink, Ltd.  
Marubun Corporation  
Matrix Electronica  
Matsubo Electronic Components Co., Ltd.  
MICROTEK Inc.  
Multiwave Co., Ltd.  
New Mercury Industrial Corp.  
Nissei Electronics, Ltd.  
Premier Components Distribution (PCD)  
Premier Technical Sales Inc.  
Roxan Telecom Co., Ltd.  
Sequoia Technology Ltd.  
Serial Microelectronics (HK) Limited  
Shanghai Ant Electronic Co., Ltd.  
Silicon Technology Co., Ltd.  
TOMEN Electronics Corp.  
Tri-Star Group, Inc.  
Unidux Inc.  
Weikeng Industrial Co., Ltd.  
World Peace Industrial Co., Ltd.  
WPI International (HK)  
Wwes Industries Corp

**HDCP Content Participant Agreement**

The Walt Disney Company  
Warner Bros.